

REMARKS

The Applicants request reconsideration of the rejection.

Claims 30 and 31 remain pending.

Claims 30 and 31 are provisionally rejection on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 22 and 23 of copending Application No. 11/936,130. At this time, the Applicants will not file a terminal disclaimer because claims 30 and 31 are allowable in view of the above amendments and the following remarks. Pursuant to Manual of Patent Examining Procedure §804(I)(B)(1) and §1490(V)(D), the double-patenting thus should be withdrawn.

Claims 30 and 31 stand rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. In reply, the Applicants note that amended claim 30 does not contain the language found by the Examiner to be unsupported by the written description, although there is support, at least, in Fig. 3 and the associated description (see pages 22-25). For example, in the layered structure model shown in Fig. 3, a user ID 31 is located at the highest priority position and terminal attribute information 35 and 36 is located at the lowest priority position. As described in the second paragraph of page 24, the terminal attribute information indicates, for example, on-line status, communication status and the like of the individual terminal. "Communication capability information" is thus described.

Further, page 25 (referring to Fig. 4) describes vertical relations that exist among permissions to be set for the object information items, and a presence server 1 that stores information indicative of the layered structure model in an object vertical relation definition table 23 of the memory 22 shown in Fig. 2. The presence server 1

stores a permission 41 for the user ID as a highest layer permission and a permission 46 for terminal attribute information as a lower layer permission, as described in the second paragraph of page 25. "Vertical relation information indicating that access permission information for said identification information has higher priority than access permission information for said communication capability information " is thus described.

Amended claim 30 fully complies with the written description requirement as well. See, for example, Figs. 3-9 and the associated description.

Claims 30 and 31 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Gavrilu, U.S. Patent Publication No. 2002/0026592 (Gavrilu) in view of Applicant Admitted Prior Art (AAPA). The Applicants traverse as follows.

A server according to claim 30 comprises a memory unit which is configured to store:

(A1) a first object information item including identification information of one of the user terminals,

(A2) a plurality of second object information items including plural kinds of attribute information relating to the user terminal or a user of the user terminal, and

(A3) hierarchical access permission setting values corresponding to a plurality of access operations having different priority levels and predefined for each of said first and second object information items,

(B) said first and second object information items being stored in association with vertical relation information to form a layered object structure for categorizing said second object information items in hierarchical relation and indicating that said first object information item has the highest permission priority and each of said

second object information items has higher permission priority than that for the other second object information items at a lower position in the layered object structure.

The server further comprises a controller, connected to the memory unit and a network interface, for controlling access operations requested to one of the first and second object information items based on the hierarchical access permission setting values, wherein:

(C1) the controller operates, in response to “a request for changing the access permission setting value” of a specific one of said access operations for a specific one of said second object information items “from a non-permission state to a permission state” received through said network interface, so as to rewrite access permission values of access operations each having a priority level equal to or higher than that of said specific access operation into the permission state for said specific second object information item and at least one of said first and (the other) second object information items each having a hierarchical relation with the specific second object information item and having permission priority higher than that of the specific second object information item in said layered structure; and

(C2) the controller operates, in response to “a request for changing the access permission setting value” of said specific one of said access operations “from the permission state to the non-permission state” received through said network interface, so as to rewrite access permission values of access operations each having a priority level equal to or lower than that of said specific access operation into the non-permission state for said specific second object information item and the other second information items each having a hierarchical relation with the specific

second object information item and having permission priority lower than that of the specific second object information item.

The Applicants note that the server of the present invention stores (A3) hierarchical access permission setting values corresponding to a plurality of access operation having different priority levels and predefined for each of first and second object information items forming a layered structure, and the server receives a request (C1, C2) for changing the access permission setting value of specific one of access operations for a specific one of said second object items from a non-permission state to a permission state or from the permission state to the non-permission state.

Turning to Gavrilă, the pre-grant publication relates to an automatic permission management method in a Role-Based Access Control (RBAC) system.

An RBAC system provides permission for objects to roles rather than directly to individual users, and controls users' permissions by granting or revoking membership to appropriate roles (see paragraph [0005]). As described in paragraphs [0007] and [0008], RBAC supports two types of role hierarchies: "role-membership inheritance" and "role-permission inheritance." In role-membership inheritance, for example, role r2 inherits the membership of role r1 if all the user members of role r1 are also members of role r2. In role-permission inheritance, role r1 also inherits role r2 if all the permissions of role r2 are also permissions of role r1.

Gavrilă indicates in paragraph [0010] that changes of role-permission hierarchies include (1) changes of role-permission inheritance, (2) creation and

registration of new objects and assignment to roles, or object deletion and de-registration, and (3) distribution and revocation of permission to roles.

The Applicants note, however, that none of the role-permissions (1)-(3) corresponds to an access permission value of a specific access operation for a specific object information items. Specifically, Gavrilă's controller of role-permission (hierarchical) changes does not correspond to the claimed controller that "operates, in response to a request for changing the access permission setting value of a specific one of said access operations for a specific one of said second object information items from a non-permission state to a permission state received through said network interface, so as to rewrite access permission values of access operations each having a priority level equal to or higher than that of said specific access operation into the permission state for said specific second object information item and at least one of said first and second object information items each having a hierarchical relation with the specific second object information item and having permission priority higher than that of the specific second object information item in said layered structure."

More in depth, Gavrilă proposes a role-based access control system including a directed acyclic graph representing role-permission inheritance relationships, disclosed as useful for associating each role with a set of abstract objects accessible to the role (see paragraph [0019]).

Further, Gavrilă proposes in paragraph [0026] to perform automatic distribution of permissions on object instances to role instances whenever (4) new roles are added to the directed acyclic graph, (5) a new role instance is created for a

role on a host computer, (6) a new object instance is created for an abstract object on a host computer, and (7) a new permission is granted to a role.

In paragraph [0027], cited in the Office Action, Gavrilă generally proposes to perform "automatic revocation and recalculation" of permissions on object instances for role instances whenever (8) permission-inheritance relations among roles are removed, (9) roles are removed, (10) an abstract object is removed, and (11) a permission is revoked from a role.

The Applicants note that these changes (4)-(11) also do not correspond to the "changing the access permission value of a specific one of access operations for a specific one of second object information items" of the present invention, because these changes (4)-(11) have no relation to partial change in an existing access permission predefined for one of existing object information items.

For example, referring to Figs. 2-7 of the pre-grant publication, while Gavrilă discloses that each role (or a role instance) can inherit abstract permissions of its descendant roles and that users (u1, u2, u3 in Fig. 3) can be registered as members of specific role instances, Gavrilă fails to suggest the features of rewriting access permission values of access operations in the upward direction on the layered structure (C1) and in the downward direction on the layered structure (C2) as performed by the present controller.

For these reasons, it is apparent that Gavrilă does not disclose the subject matter of (A1) - (A3), (B), and (C1) - (C2), and particularly (A3), (B), and (C1) - (C2). Even the combination of Gavrilă with the alleged AAPA does not disclose the features, as AAPA fails to supply the teachings missing from Gavrilă.

Moreover, paragraph [0027] simply does not teach with sufficient specificity the limitations of the claims against which it is asserted. The Office Action is scanty in asserting that

"automatically changing permissions-inheritance relations when a permission is revoked"

anticipates the previously-claimed

wherein said controller operates, in response to a request for changing the access permission setting value of a specific one of said access operations for said communication capability information from a non-permission state to a permission state received through said network interface, so as to rewrite access permission values of access operations each having a priority level equal to or higher than that of said specific access operation into the permission state in both said identification information and said communication capability information; and operates, in response to a request for changing the access permission setting value of a specific one of said access operations for said identification information from the permission state to the non-permission state received through said network interface, so as to rewrite access permission values of access operations each having a priority level equal to or higher than that of said specific access operation into the non-permission state in both said identification information and said communication capability information.

One easily sees that the amended language is also not met by Gavril's paragraph [0027].

Claim 31 is also rejected as noted. Claim 31, however, inherits the patentability of independent claim 30 from which it is derived and is thus patentable. Therefore, for brevity, the Applicants will not argue its separate patentability at this time.

In view of the foregoing amendments and remarks, the Applicants request reconsideration of the rejection and allowance of the claims.

To the extent necessary, the Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to

the deposit account of Brundidge & Stanger, P.C., Deposit Account No. 50-4888
(referencing attorney docket no. NIT-415).

Respectfully submitted,

BRUNDIDGE & STANGER, P.C.

/Daniel J. Stanger/
Daniel J. Stanger
Registration No. 32,846

DJS/sdb
(703) 684-1470